# Improving the Security of E-Passports with WDDL Logic and Elliptic Curve Cryptography

N.Sivasankari
Department of ECE,
Kalasalingam University
Virudhunagar, Tamilnadu, India

M.Kannan
Special Officer of Distance Education
Annamalai University
Virudhunagar, Tamilnadu, India

***Abstract*— This paper describes the security of E-passport with elliptic curves. The chip which is having the information about the passenger should occupy very less area & The chip information cannot be traceable. AS Compared to other public key cryptosystems such as AES and DES elliptic curve cryptography provides greater authentication and verification security. Contactless smart cards work only with ECC because other systems require too much induction energy. The physical implementations such as power consumptions should not allow the hacker to think about the private key information. Hence in FPGA technology WDDL logic can be used to prevent the hackers even though it consumes more power.**

***Keywords*- PACE; Galois field; Elliptic Curves; WDDL logic.**

## I. Introduction

An electronic passport should securely store biographical information and digital image that are identical to the information that is visually displayed in the passport. Contactless chip technology allows the information stored in an Electronic Passport to be read by special chip readers at a close distance; and digital signature technology is used to verify the authenticity of the data stored on the chip. This technology is commonly used in credit cards and other secure documents using integrated circuits or chips. The Electronic Passport facilitates traveler by allowing greater border protection and security. The information stored on the chip must be prevented from being altered. For this public key infra structure is used. The e-passport and the use of the PKI digital signature stands to benefit the legitimate traveler. For providing Security& Authentication one of the public key cryptosystem (i.e) elliptic curve cryptography can be used because of its security in lesser no of bits. Efficient finite field multiplication is crucial for implementing public key Cryptosystem. Elliptic curve cryptography (ECC) has been widely adopted in modern security standards to provide robustness for secure data transaction such as personal identity verification (PIV), data and finance authentication, digital signature, and security key management, etc. With the unified architecture for both prime field and binary field cryptosystems, Information related with the physical implementation of the device, such as time delay and power consumption, has been used repeatedly to find the secret key in so-called Side Channel Attacks.

### A. Attacks

#### 1) Wireless E passports introduces two new security risks:

##### a) Active scanning attacks

An attacker communicates with the passport without the owner’s consent, by bringing a reader in close proximity to the passport, e.g. when the passport is in a coat pocket or a handbag.

##### b) Passive eavesdropping attack

An attacker eavesdrops on the communication when the passport communicates with a legitimate reader with the owner’s consent, for instance at passport control at an airport. The resulting lookup table from government allows an attacker to determine where a chip is from.

#### 2) Using RFID tags

The Basic Access Control protocol ensures that the data on the e-passport can only be read by someone who knows the key derived from the date of birth, date of expiry and number on the passport. Our attack lets someone who does not know this key trace a passport, i.e., if an attacker can observe a run of a particular passport then they can build a device that detects whenever the same passport comes into range of the reader. RFID tags receive their power via a signal from the reader; FCC regulations [FCC] limit the power of the readers, leading to an effective range of about 9cm.

#### 3) Threat to hack Digital Signature Algorithms

For messages sent through a non-secure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital signatures are equivalent to traditional handwritten signatures in many respects, but properly implemented digital signatures are more difficult to forge than the handwritten type. With Try and Implement Algorithm the hacker may find the number.

### B. Elliptic curves

An elliptic curve is a plane curve which consists of the points satisfying the equation.

$$y2 = x3 + ax + b \qquad (1)$$

The constants values a& b must satisfy the condition $4a3+27b2 \neq 0$ together with a point at infinity. The addition of two points of this curve can be defined to form a group.

In binomial Galois filed operation is defined as Polynomial: $(x6 + x4 + x + 1)+(x7 + x6 + x3 + x) = x7 + x4 + x3 + 1$

Binary:{01010011}+{11001010} = {10011001}

Hexadecimal: {53} + {CA} = {99}

Elliptic curves are interesting for cryptography is that the discrete logarithm problem in that group is believed to be computationally hard. This means that elliptic-curve-based protocols can use shorter keys and more efficient arithmetic than protocol based on other groups such as nonzero integers modulo a prime number.

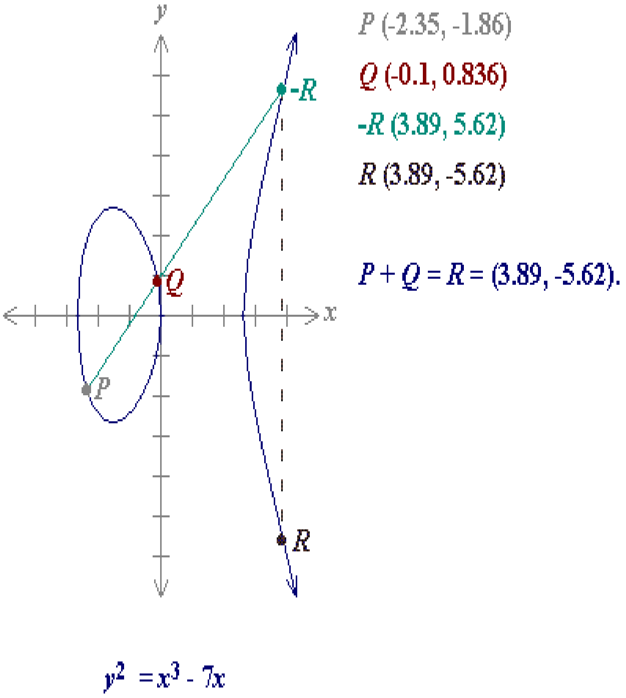

Figure 1. ECC Addition

### C. WDDL

Wave dynamic differential logic combined with differential routing is a working, practical technique to thwart side-channel power attacks. Measurement-based experimental results show that a differential power analysis attack on a prototype IC, fabricated in 0.18µm CMOS, does not disclose the entire secret key of the ECC algorithm at measurement acquisitions. This makes the attack infeasible. The required number of measurements is larger than the lifetime of the secret key in most practical systems.

Side-channel power attacks can be mounted on ASICs, FPGAs, DSPs and microprocessors because in standard CMOS technology, power is only drawn from the power supply when a 0 to 1 output transition occurs. Therefore, by measuring the power supply current during the encryption, and then performing statistical analysis of the measured power traces, the secret key can readily be determined. The secure digital design flow pursues constant power dissipation by balancing the power consumption of the logic gate. When the power dissipation of the smallest building block is constant and independent of the signal activity, no information is leaked through the power supply. As a result, it protects against all power attacks including simple power analyses, differential power analyses and higher order power analyses.

## II. The Encoding problem-Relevant work

Binary finite fields (Galois Field ($2^m$)) provide efficient algorithms and implementations of the arithmetic operations. For example, additions and subtractions in GF($2^m$) are very fast because they can be implemented as simple XOR operations without carry propagation. This renders these fields very favorable for cryptographic applications with long key lengths. Several elliptic curves that are for example recommended for ECC by the National Institute of Standards and Technology use these binary fields.

The calculation of points on elliptic curve over finite fields is described in [2]. The methods to construct points on an elliptic curve were explained in [3] & [4]. These results have prompted further research in this area as well as various cryptographic applications. For this purpose, they proposed a very natural way to encode values to that curve. However, this works only for curves of a special form (super singular curves), which aren't suitable for most applications owing to security properties.

## III. Password-Authenticated Communication Establishment

The International Civil Aviation Organization (ICAO) maintains a series of specifications pertaining to secure communication between the chips on Machine-Readable Travel Documents (MRTDs) and MRTD readers. PACE(Password Authenticated Communication Establishment) aims to establish a secure communication channel between a chip and terminal sharing a password p. For e-passports, this password is obtained from the MRTD's machine-readable zone. PACE has six steps; card issuing phase, Authentication phase, Key distribution phase. After these three steps, the two parties have obtained a common high- entropy secret: point Z on the elliptic curve. The next three steps are key derivation, key confirmation, and session establishment, which are relatively standard and don't involve point encodings.

## IV. Implementations

In ECC scalar multiplication is the time consuming method of Finite point multiplication in affine Coordinates. This method uses the simple algorithm.

```
Input: P = (x, y)  x, y ε GF(2^m) and
k = (k_{m−1}, k_{m−2}, ..., k_0)
Output: R = kP
R ← (0, 0)
S ← P
for i from 0 to m − 1
if k_i = 1 R ← ECC-ADD(R, S)
end if
S ←ECC-Double(S)
End for
```

Using affine representation of elliptic curve points, the ECC-ADD operation of two points is defined as Input P = ($x_1$, $y_1$), Q = ($x_2$, $y_2$) Output R = ($x_3$, $y_3$)

$$x_3 \leftarrow \lambda_2 + \lambda + x_1 + x_2 + a$$

$$y_3 \leftarrow \lambda(x_1 + x_3) + x_3 + y_1$$

$$\lambda \leftarrow (y_2 + y_1)/(x_2 + x_1)$$

The ECC-DOUBLE operation

Input P = ($x_1$, $y_1$), Output R = ($x_3$, $y_3$)

P + P = 2P where:

$x_3 \leftarrow \lambda_2 + \lambda + a$

$y_3 \leftarrow x_2 + \lambda x_3 + x_3$

$\lambda \leftarrow x_1 + y_1/x_1$

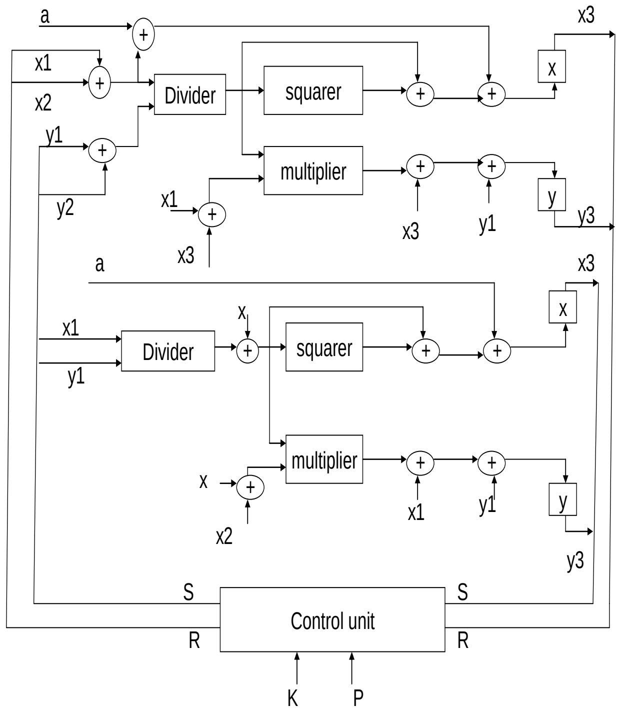

Figure 2. Architecture for ECC-ADD& ECC-DOUBLE

The algorithm used here allows flexible changes in ECC. The multiplier, divider and squarer modules can be updated just by replacing them by better performed modules. The chip technology for producing IC in E Passport can be implemented using WDDL logic.

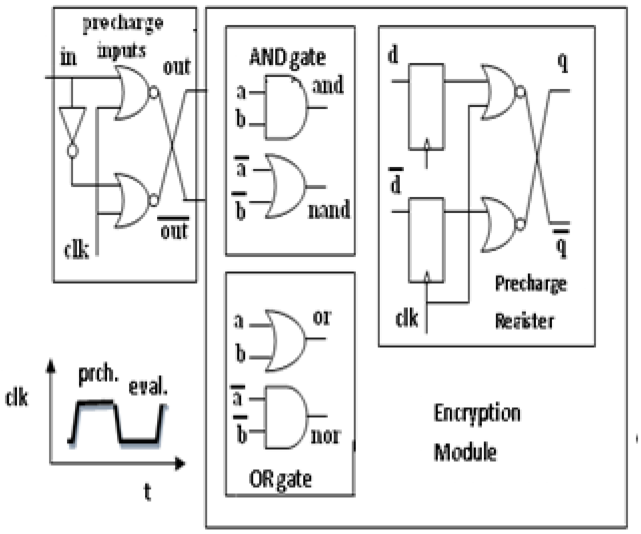

Figure 3. WDDL-Precharge wave generation.

Or by using any of the algorithms ECC processor can be constructed. The results are analyzed for this module in Xilinx as:

TABLE I. AREA/TIMING RESULTS

| Multiplier Area | Area | Cycles/ kP | Clk period (ns) | Time kP(ms) |
|---|---|---|---|---|
| Serial | 5632 (52%) | 72527 | 19.409 | 1.36 |
| D = 4 | 6762 (62%) | 52620 | 21.611 | 1.06 |
| D = 8 | 7342 (68%) | 49360 | 20.747 | 1.02 |
| D = 16 | 8537 (79%) | 47730 | 22.286 | 1.13 |
| D = 32 | 10750 (99%) | 46915 | 29.040 | 1.4 |

The individual modules compilation report taken using Quartus II with processor EP2C20F484C7.

TABLE II. LOGIC RESULTS

| Modules | Logic Elements | Logic Registers |
|---|---|---|
| Squarer | 165 | 0 |
| Divider | 218 | 132 |
| multiplier | 92 | 33 |

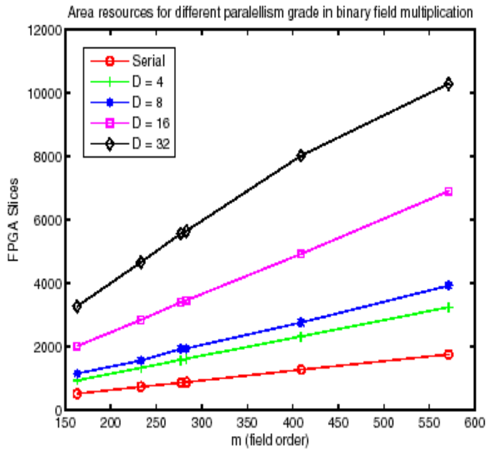

Figure 4. Area recourses for ECC multiplication for different field order.

## V. CONCLUSIONS

ECC provides better security compared to other pubic key cryptosystems mathematically. The chip designs inside the E-passport may be more resistive to prevent side channel attacks. A digit serial multiplier, division algorithm & combinatorial squaring units are used for ECC. The better modules compared to this may be used. The major contribution of this paper is a novel method to combine WDDL logic and ECC based public key cryptosystems to produce better e-pass port security systems.

## REFERENCES

[1] Hervé CHabanne *Morpho,* MeHdi TibouCHi, *École normale supérieure*“Securing E-passports with Elliptic Curves” Crypto Corner March -April 2011.

[2] R. Schoof, “Elliptic Curves over Finite Fields and the Computation vol: 44, no. 170, 1985, pp. 483–494.

[3] A. Shallue and C. van de Woes-tijne , " Construction of rational points on Elliptic curve over finite fields" Algorithmic number Theory, LNCS 4076, Springer 2006, pp. 510–524.

[4] T. Icart, "How to Hash into Elliptic Curves," Advances in Cryptology—Crypto 2009, LNCS 5677 Springer, 2009, pp. 303–316.

[5] D. Boneh and M.K. Franklin "Identity-Based Encryption from the Weil Pairing," Advances in Cryptology—Crypto 2001, LNCS 2139, Springer, 2001, pp. 213–229.

[6] D. Brumley and D. Boneh, "Remote Timing Attacks Are Practical," Computer Networks, vol. 48, no. 5, 2005, pp. 701–716.

[7] R.R. Farashahi, I.E. Shparlinski and J.F. Voloch, "On Hashing into Elliptic Curves," J.Math- ematical Cryptology, vol. 3, no. 4 2010PP.353-360 ww.mautexas.edu/users/voloch/ Preprints/hashing.pdf

[8] P.-A. Fouque and M. Tibouchi, "Estimating the Size of the Image of Deterministic Hash Functions to Elliptic Curves," Progress in Cryptology—Latincrypt 2010, LNCS 6212, Springer, 2010, pp. 81–91

[9] Supplemental Access Control for Machine Readable Travel Documents ver. 1.01, tech. report, Int'l Civil Aviation org Nov 2010,www2.icao.int/en/MTRD /Downloads /Technical%20 reports/technical%20reports.pdf.

[10] S.M. Bellovin and M. Merrit,"Encrypted key exchange" Password-Based Protocol Secure against Dictionary Attacks," Proc. Symp. Research in Security and Privacy, IEEE Press, 1992, pp. 72–84.

[11] E. Brier et al., "Efficient Indifferentiable Hashing into ordinary Elliptic curves" Advances in Crypto 2010 LNCS 6223, Springer, 2010, pp. 237–254.

[12] J. Bringer, H. Chabanne, and T. Icart, "Password Based Key Exchange Protocols on Elliptic Curves Which Conceal the Public Parameters," Applied Cryptography and Network Security, LNCS 6123, 2010, pp. 291–308.

[13] http://travel.state.gov/passport/passport_2788.html

[14] Tiri et al, Securing Encryption Algorithms against DPA at the Logic Level: Generation Smart Card Technology, CHES'03, LNCS 2779, p. 125.

[15] D. Hankerson, L. L´opez, and A. Menezes. Software Implementation of Elliptic Curve Cryptography over Binary Fields. In Proc. of the Second International Workshopon Cryptographic Hardware and Embedded Systems, CHES'2000, volume 1965 of Lecture Notes in Computer

[16] Science, pages 1–24, Worcester, MA, August 2000. Springer.

[17] Miguel Morales-Sandoval and Claudia Feregrino-Uribe," GF(2m) Arithmetic Modules for Elliptic Curve Cryptography"